



COMDTINST 5230.56

COMMANDANT INSTRUCTION 5230.56

Subj: POLICY ON COAST GUARD USE OF INTERNET/WORLDWIDE WEB

- Ref:
- (a) Paperwork Management Manual, COMDTINST M5212.12 (series)
 - (b) Public Affairs Manual, COMDTINST M5728.2B (series)
 - (c) Freedom of Information and Privacy Acts Manual, COMDTINST M5260.3 (series)
 - (d) Use of the Coast Guard Seal, COMDTINST 5030.12 (series)
 - (e) Automated Information Systems (AIS) Security Manual COMDTINST 5500.13A (series)
 - (f) CG Correspondence Manual, COMDTINST M5216.4 (series)
 - (g) Standards of Conduct Manual, COMDTINST M5370.8A (series)
 - (h) Authorized Use of Government Telephone Systems, COMDTINST 2060.3 (series)
1. **PURPOSE.** This Instruction promulgates policy in the areas of Coast Guard Internet site management, page content, page development, and usage.
 2. **ACTION.** Area and district commanders, commanders of maintenance and logistics commands, commanding officers of integrated support commands, commanding officers of Headquarters units, Assistant Commandants for directorates, chief counsel and special staff elements at Headquarters shall ensure compliance with the provisions of this directive.
 3. **DIRECTIVES AFFECTED.** COMDTINST 5230.1 dated 26 December 1995 is hereby canceled.

4. **DEFINITIONS.** As used in this Instruction, "Assistant Commandant" means all Assistant Commandants, Chief Counsel, and the chiefs of all special staff elements. Additional definitions include:
- a. Webmaster - an individual responsible for the technical management of a program or subordinate unit web site, for maintaining currency of that web site, for submitting a registration form and for posting information to the web site.
 - b. Hyperlinks - buttons or words located on the page that take the user to other places within the document or other pages (similar to bookmarks in MS Word) as well as access other files and other web sites.
 - c. Server - computer that provides files or applications to a user's computer. In the case of the Internet, this is the machine that provides the files requested by the browser application (Internet Explorer) running on the user's CGSWIII.
 - d. Internet - a worldwide series of inter-connected computer networks that evolved from a 1950's Department of Defense project called ARPANET.
 - e. HTML - hypertext markup language. The language used to write world wide web pages.
 - f. Content Author - originator of HTML page.
 - g. Content Approving Official - individual who approves HTML content for posting to the world wide web (WWW) server.
5. **BACKGROUND.** The Internet and its World Wide Web provide the Coast Guard unprecedented opportunities to improve ways of doing business. Areas where this technology may be applied to improve service and reduce costs include, but are not limited to: distribution of targeted business information to customers; interactive information exchange with customers; distribution of Coast Guard specific information to personnel unable to directly access the Coast Guard Data Network (CGDN) (i.e. Reserve members, Auxiliary members, active duty personnel in special assignments, etc.); Coast Guard military and civilian employment opportunities; increased public awareness of Coast Guard missions, reduction of postal costs and much more. Since being established as a prototype in 1995, the Coast Guard's World Wide Web (WWW) pages have grown to provide a significant amount of information. Visits to the site (called "hits") have increased from only a few hundred per month to well over 1.25 million hits per month. This is but one measure of the rapid growth this medium is experiencing as it becomes an integral part of business operations worldwide. Use of the Internet will allow us to keep pace with the best that technology has to offer, ultimately improving CG mission performance worldwide.

6. **DISCUSSION.** ALDIST 018/97, Policy on USCG World Wide Web (WWW) Content provided initial guidance about Internet content, WWW page development, and Internet use to distribute Coast Guard information. This instruction clarifies and expands on the information previously provided in that reference and in several other messages, and specifies the responsibilities of various organizational elements for management and use of the WWW.
- a. **Current Status.** The Coast Guard maintains information on the WWW at several sites. The largest share of WWW information is currently posted on a DOT-owned server. Other sites include: the Coast Guard Navigation Center (NAVCEN) which maintains its own server via contract; Training Center Petaluma which maintains its own server; R&D Center which maintains its own server; Coast Guard Institute which posts information to a commercial server with a database interface; National Data Buoy Center (NDBC) which posts information on a National Oceanographic Administrative Agency (NOAA) server; Container Inspection Training Assistance Team (CITAT) which posts information to a local DOT server; the Coast Guard Auxiliary which hosts information across several servers; and several districts and units which currently post information on commercial servers.
 - b. **Planned Transitions.** All Coast Guard WWW information currently posted at various sites (excluding Auxiliary) will be moved to the new Coast Guard server site located at Operations System Center (OSC) in Martinsburg, West Virginia. This transition began in October 1997. Plans are to copy information posted on the DOT server and other sites. After all of the information has been mirrored at the site, the directory structure will be rebuilt and existing files relocated to conform to the new structure to allow better management of the site. After a suitable test period, all references to Coast Guard WWW information will reflect the new location. Web pages at old sites will be modified to reflect their new locations. Users with advanced browsers will be auto-forwarded to the new site. After one year, all information and forwarding pages at old server sites will be removed and only the OSC server will host U.S. Coast Guard Web pages. Stand-up of the new server as well as the transition of information from other servers is being managed by the Telecommunications and Information Systems Command (TISCOM).
 - c. **Server Access.** Concurrent with the new server being brought on line, the process of assigning access authority to appropriate organizational elements will take place and information may be posted to the server by authorized personnel (see responsibilities section below).
 - d. **WWW Addresses.** Addresses at the new server will take the form: www.uscg.mil. Even though organizational elements will reside below this level, our Windows NT-based server will allow alias names to be assigned to major programs and units provided there is a business need for such an alias. So, for example, Coast Guard Reserve may request to use the address: www.uscg.mil/reserve even though the actual location might be: www.uscg.mil/g-w/g-wtr/reserve.

- e. Funding. Commandant (G-SI) shall identify funding for the baseline services at OSC. Baseline services are defined as providing the same internet services currently provided by DOT. Current cost estimates are:

Item	Costs
PERSONAL COST (2 WEBMASTERS)	\$ 200,000
TECHNOLOGY COSTS/RECAPITALIZATION	\$ 50,000
TOTAL	\$ 250,000

Any additional costs and/or capabilities shall be brought to the Internet Configuration Control Board (ICCB), defined below in paragraph 7.c, for approval and identification of funding sources.

7. **RESPONSIBILITIES.**

- a. General. The Coast Guard Internet is overseen by the Internet Configuration Control Board (ICCB) under the Coast Guard's Chief Information Officer (Commandant (G-SI)) within the Systems Directorate, Commandant (G-S) at Coast Guard Headquarters. Responsibility for content and access to the Internet for posting information is delegated to and resides within (listed in order of responsibility for managing web content):

- (1) Programs (as overseen by Assistant Commandants at the Headquarters level)
- (2) Areas/MLCs
- (3) Districts/ISCs
- (4) Units/Commands

Organizational elements given the authority in this instruction may elect to establish and maintain a presence on the Internet; if the decision is made to pursue the use of this medium, the guidelines in this instruction (enclosures 1-11) shall be followed. The posted information shall conform with the policies outlined in references a-g.

- b. Chief Information Officer (CIO). The Coast Guard's Chief Information Officer has ultimate authority for all matters relating to use of the Internet. Assigned within the Systems Directorate, the position is held by the Director of Information and Technology, Commandant (G-SI). The CIO, with input from the Internet Configuration Control Board, is final authority for:

- (1) Assigning access authority for posting information to the Internet.
 - (2) Setting minimum levels of competence for webmasters and content managers.
 - (3) Establishing standard software for web authoring and publishing.
 - (4) Brokering any disputes which may arise regarding Internet policy.
- c. Internet Configuration Control Board (ICCB). The ICCB is composed of representatives from each of the Assistant Commandants, the Chief of Staff, the Chief Counsel, as well as representatives from Public Affairs Commandant (G-CP), OSC, TISCOM, LANTAREA, PACAREA, and Auxiliary. The ICCB recommends policies for administering and managing the Coast Guard's use of the Internet to the CIO.
- d. Assistant Commandants. The Assistant Commandants hold primary responsibility for information posted to the Internet for their areas of responsibility (AOR). Each is responsible for designating a program-level webmaster (see enclosures 1, 4, and 6 on qualifications, roles, and responsibilities of webmasters and content providers) and for assigning subordinate control within their program to directorates and offices at the headquarters level; to area/MLC-level program elements; to district/ISC-level program elements; and other subordinate organizational elements as needed. They may establish specific policies for use of the Internet for organizational elements under their control and provide access for posting information by those subordinate elements. They may post information, provide links, and establish new information services within technological limitations provided they adequately resource such expanded services. Programs have the highest level of authority for allowing posting access to subordinate elements and for posting information related to their area of responsibility. They may delegate this authority to lower-level program elements or to lower levels of the chain of command.
- e. Public Affairs (Commandant (G-CP)). While providing information to Coast Guard customers is primarily a program function, the use of the Internet, with its ability to reach a vast audience, can tremendously impact public response to the Coast Guard. A service-wide approach to external communications with key customer groups can improve overall organizational performance by transforming current practice into a more coordinated, effective, and efficient approach. To that end, Public Affairs will:

- (1) Ensure that a consistent Coast Guard message is delivered to all customer audiences.
 - (2) Provide Assistant Commandants, area commanders, MLC commanders, and district commanders support in identifying key customers as needed.
 - (3) Establish strategic content standards and appearance guidelines for information posted on the Internet, consistent with a Coast Guard-wide approach to all media.
 - (4) Set standards for style and appearance of information posted to the Internet in collaboration with the ICCB.
- f. Areas/MLC Commanders. Area/MLC Commanders are responsible for general information posted to the Internet within their AOR. They shall appoint webmasters, post information and provide links to senior and subordinate elements, commands, and general information. They may exercise content control over programs at their level with permission of the appropriate senior program manager. Areas/MLCs may not re-publish higher level information (unless it has been modified for specific area/MLC -level purposes); links must be used to provide relevant information posted by higher levels in the chain of command.
- g. District Commanders/ISC Commanding Officers/HQ Unit Commanding Officers and Directors of HQ Units. District Commanders/ISC Commanding Officers/HQ Unit Commanding Officers and Directors of HQ Units are responsible for general information posted to the Internet within their AOR. They shall appoint webmasters, post information and provide links to senior and subordinate elements, commands, and general information. They may exercise content control over programs at their level with permission of the appropriate senior program manager. To avoid duplicative effort, redundancy and possible end-user confusion, no organizational element may re-publish higher level information (unless it has been modified for their specific purposes); links must be provided to relevant information posted by higher levels in the chain of command.
- h. Unit Commanders/Commanding Officers. Unit Commanders/Commanding Officers, if given authority by their chain of command, are responsible for general information posted to the Internet within their AOR. They shall appoint webmasters, post information and provide links to senior and subordinate elements, commands, and general information. They may exercise content control over programs at their level with permission of the appropriate senior program manager. No unit may re-publish higher level information (unless it has been modified for specific unit/command-level purposes); links must be provided to relevant information posted by higher levels in the chain of command.
- i. Telecommunications and Information Systems Command (TISCOM). TISCOM, in coordination with designated personnel at Operations

System Center (OSC) is responsible for management of the physical infrastructure and support of the Coast Guard Internet server. In this role, they are primarily responsible for security of the server and related systems; system users (especially designated webmasters) also have significant responsibility for the security of the Coast Guard Internet and are guided by reference (c) with respect to these issues.

- j. All Users. All users who elect to transact Coast Guard business via the Internet must ensure that the policies and procedures in reference (a) are followed. Users should note that conducting business via the Internet does not eliminate the existing requirements for ensuring that some form of data archiving is in use since official records are being created. Additionally all users will be held accountable for ensuring their proper use of the Internet and that any content developed by them supports a valid business need.

8. **POLICY.**

a. Internet WWW Information Management.

- (1) Assistant Commandants, area commanders, MLC commanders, HQ unit commanding officers and district commanders are authorized to establish and maintain a presence on the Coast Guard Internet site for the dissemination of Coast Guard information and to conduct Web-based Coast Guard business specific to their Area of Responsibility (AOR). Those organizational elements maintaining a presence on the CG Internet site shall formally designate an Internet Webmaster and an Internet Content Approval Official (may be the same individual). Waivers for use of non-Coast Guard servers may be submitted to the ICCB for consideration. Waiver requests must clearly indicate why the Coast Guard server is inadequate for specific business reasons. Note that when considering a waiver request, the Coast Guard server is a fully scaleable system which may be modified or augmented to address specific user requirements.
- (2) A webmaster is an individual responsible for the technical management of a program or subordinate unit web site, for maintaining currency of that web site, for submitting a registration form and for posting information to the web and to ensure posted information is accurate and current. Enclosure (1) outlines qualifications, roles, and responsibilities of Coast Guard webmasters and content providers.
- (3) The Internet shall be used to publish Coast Guard information as well as to conduct Coast Guard business with external customers. Information and business with Coast Guard

personnel (active, reserve, civilian, auxiliary, contract) may also be conducted via the Internet provided that there is no suitable internal communications medium available, that all other guidelines for distribution of information to the public are adhered to and that appropriate security measures are employed as needed. Content approving officials need to be cognizant of the unique nature of the WWW: any posted information is immediately accessible by all WWW users (currently estimated at over 60 million people) throughout the world. All policies and procedures which apply to hard copy clearance also apply to publication of materials on the Internet.

- (4) Assistant Commandants, area commanders, MLC commanders, district commanders, and unit commanding officers desiring to provide Coast Guard information or records via an Internet web page shall establish a release procedure to ensure that the records have been carefully reviewed and comply with the policies and procedures established in references (a) through (g).
- (5) All initial references to the service on the Internet shall use either the form "United States Coast Guard" or "U.S. Coast Guard."
- (6) All CG Internet sites must submit a completed registration form to the ICCB. The registration form (see enclosure 10) will provide accountability and essential information required to manage the Coast Guard WWW site and shall be updated and resubmitted as necessary.
- (7) Publish only official descriptions of CG missions and entities. Include the name of the approving official and the effective date when posting official instructions.

b. Security.

- (1) Each web site shall ensure that the requirements identified in reference (e) are satisfied through the implementation of selected managerial, administrative, and technical procedures. In addition, systems must also provide the capability to detect and/or negate attempts to circumvent system protection. Security control measures will cover the following areas:
 - (a) Management controls
 - (b) Acquisition, Development, and Installation Controls
 - (c) Operational Controls
 - (d) Security Awareness Training
 - (e) Controls over the Security of Applications

- (2) The Coast Guard Internet server will contain various technical controls such as unique user identification and authentication codes, incorrect log on attempt notification, and passwords to protect the system.
- (3) Only individuals with authenticated user IDs will have access to the system and its resources. In addition, systems administrators shall define and control the access of subjects (e.g., user, groups) to objects (e.g., directories, files, resources) using an appropriate access right based on their level of need (e.g., the right to only read files, read and/or write files, or the right to read, write and run executable files within a given directory).
- (4) Access controls shall be used to prevent unauthorized access into sensitive or other systems areas.

c. Internet Web Page Content.

- (1) Coast Guard Internet web sites shall be used to publish appropriate information as well as to conduct official CG business with external Coast Guard customers. Coast Guard web sites shall not be used for the private gain of individuals, e.g. posting of resumes.
- (2) Content disclaimers shall be used and content must be officially approved. The Department of Transportation disclaimer policy will be used as soon as it is completed (estimated to be March 1998). All pages shall provide links to a local copy of this policy once it is available. All policies and procedures which apply to hard copy also apply to publication of materials on Coast Guard Internet web sites.
- (3) No payment of any kind shall be accepted to provide a link on any Coast Guard web page to another web page or to provide specific content on a Coast Guard web page.
- (4) Requests for identical information from ten or more members of the public must be approved, prior to use, as noted by reference (a). This includes surveys using check box, radio button or text form fields. Approval is not required for forms which ask for general solicitations of comments such as opinion-based feedback forms and e-mail links.
- (5) Usage statistics may be compiled. However, requests for identifying information that could be considered a survey and/or "cookies" (small data files contained in a user's browser that provides information about that user to the web site server) shall not be collected unless authorized by the ICCB.
- (6) Any information requested from the public shall include an explanation of how the requested information is intended to be used.

- (7) Web sites desiring to provide CG information or records via a Coast Guard Internet web page shall establish procedures to ensure that the records have been carefully reviewed and comply with all applicable policies and procedures per the provisions of reference (c). On openly accessible web pages, do not release:
 - (a) Personal opinion or agenda
 - (b) Internal Program Agenda not appropriate for general distribution (note: Internal program agendas not appropriate for general discussion can be posted to access-controlled pages or on the CG Intranet (CGWEB). These pages are not intended for classified material but provide the equivalent level of protection as Windows NT does for files.)
 - (c) Inflammatory comments
 - (d) Information protected under the Privacy Act
 - (e) Classified information
 - (f) Procurement-sensitive/proprietary information
 - (g) Copyrighted or trademarked material
 - (h) Information which would interfere with an official investigation or law enforcement (LE) activity, or judicial proceeding, including information which could subject LE personnel to potential harm
 - (i) Pre-decisional information, reader files, internal letters and memoranda shall not be released unless approved by the appropriate authority
- (8) Information currently disseminated via external newsgroups, electronic bulletin boards, and/or electronic mail lists, shall be converted to the web format wherever practical.
- (9) Webmasters shall provide hyperlinks (buttons or words located on the page that take the user to other places within the document or other pages) to needed information rather than duplicating information or files. Duplicate information shall be consolidated by the senior command, including graphical elements. Additional direction will be provided by cognizant programs, as needed.
- (10) Information under the purview of specific programs is considered to be "owned" by those programs and shall not be posted by organizational elements other than those programs.

Also, hierarchical program information shall be posted by the appropriate organizational element (i.e. high-level policy information will be posted by Assistant Commandants, information specific to local implementation will be posted by areas, MLCs, districts, or units). Hyperlinks to information vertically and horizontally within the organization are strongly encouraged to provide links to higher levels of background information, lower levels of implementation information, and horizontal or cross-organizational links to related information.

- (11) USCG WWW pages that do not conform to the standards outlined in this instruction will either be modified or removed, at the discretion of the Internet Configuration Control Board (ICCB).
- (12) Official federal government content is in the public domain. Use of the copyright designation is inappropriate and shall not be used.

d. Web Page Development.

- (1) Commandant (G-CP) shall maintain the content of the "United States Coast Guard Home Page" and its page links in collaboration with the ICCB.
- (2) The ICCB shall establish broad guidelines for page layout and common graphic elements as well as for other required page elements. Assistant Commandants, area commanders, MLC commanders, and district commanders shall be allowed artistic creativity in developing their web pages within those guidelines. Suggested web page templates will be provided by the ICCB in order to establish a consistent Coast Guard presentation. Organizational elements may, within the broad guidelines established by the ICCB, establish a template to provide common appearance of pages within their program. Enclosure (2) provides a description of page layout guidelines and required page elements.
- (3) Links to pages outside the Coast Guard are authorized in support of valid business objectives and must be approved by the content approving official. Links may not endorse a particular non-Governmental product or service or provide preferential treatment. All pages shall include a local copy of the Department of Transportation standard disclaimer is developed. In the interim, pages containing links to external pages shall use the following disclaimer: "Links from these pages (or "this page" on a specific page of links) to non-Coast Guard sites are provided as a customer service and do not represent any implicit or explicit endorsement by the United States Coast Guard of any commercial or private issues or products presented
- (4) As outlined in reference (d), the Coast Guard Seal (with gold braided rope) shall not be used on Coast Guard web pages.

- (5) Commercial advertising on Coast Guard web pages is prohibited.
- (6) All sound, graphic and motion content shall have a text alternative so that visually impaired users may access the content with a text reader.
- e. General Usage. The Internet shall be used to support a valid, business needCoast Guard. It shall not be used for personal, political, moral or philreasons. Official government computer systems are subject to security moniat all times, and the use of such systems constitutes consent to CommunicationsSecurity (COMSEC) monitoring. If security monitoring revealsimproper or criminal activity, such evidence will be provided to appropriate management and/or law enforcement personnel.
 - (1) Supervisors shall ensure that their employees comply with this instruction. Use of the Internet is also governed by the policies set forth in reference (h). Subject to the discretion of each Command, employees may use the internet in the same manner as permitted in reference (h), e.g. electronic mail message to spouse or child.
 - (2) Users shall not engage in inappropriate use of the Internet. Inappropriate use of the Internet may result in disciplinary action. Inappropriate use is the personal use of the Internet for entertainment, non-business purposes and includes, but is not limited to: downloading programs without authorization, opening any downloaded files without first utilizing an anti-virus utility to check the files, engaging in illegal activity (e.g. child pornography, violation of the Uniform Code of Military Justice by military members), gambling, playing games, participation in non-business related chat room and surfing the net for personal, non-business information such as favorite hobbies, sports statistics and financial investment information.
- f. Forms Availability. The Coast Guard Internet Registration Form, CG-5641, is contained in this Instruction as enclosure (9). It will also be available via the world wide web from the Coast Guard Homepage located at <http://www.uscg.mil>.

/s/ George N. Naccara
Director of Information
and Technology

Encl: (1) Webmaster Job Description
(2) Coast Guard Internet Style Guide
(3) Coast Guard Internet Security Plan
(4) Coast Guard Internet Training Plan

- (5) Government Information Locator Service (GILS) requirements
- (6) Coast Guard Internet Support Plan
- (7) Coast Guard Internet Configuration Management Plan
- (8) Web Site Measurement Guidelines
- (9) Coast Guard Internet Registration Form
- (10) Internet Process Flow Char

CG WEBMASTER Job Description

MANAGEMENT:

Manages a website and homepage for an Assistant COMDT, Area, MLC or District.
Mediates technical issues between content authors and system administrators.
Supports or delegates webmaster support for all authorized subordinate web sections.
Works with WWW content authors to ensure effectiveness, consistency and timeliness
Develops, enforces and takes responsibility for the quality and style of the site in compliance with this Internet Instruction.
Suggests technical strategies to create and maintain web content and design technologies to improve effectiveness.
Plans, develops, deploys, manages, maintains and assures security of the web site.
Interfaces effectively with senior management and diverse user groups to include oral presentations, and written reports. In addition, demonstrates good negotiation skills, and excellent analytical skills.
Operates within, and enhances a team environment.
Provides input to the ICCB to help ensure that the Coast Guard is effectively utilizing web technology as a business tool.
Maintains updated WWW site registration and forwards copy to ICCB.

TECHNICAL:

Serves as technical contact for AOR, and posts content to WWW server.
Ensures that applicable standards such as HTML and link validity are met.
Optimizes the web architecture for navigability.
Provides user support and training, construction, and file transfer of web pages.
Creates and maintains home page and web pages for AOR.
Stays current in technological updates, web developments, web security and computer networking.
Has working knowledge of HTML and a solid knowledge of Internet standards and protocols such as HTML, HTTP, Microsoft IIS, and CGI (or other appropriate interface) design and programming.
Maintains site usage statistics.
Reports statistical performance to content authors and content approving official.

ARTISTIC:

Creates an intuitive site that adequately reflects the site's business objective, enhancing content, while not obscuring it. Has knowledge of basic graphic design principles, marketing strategies and standard design tools, content development and management products. Creates effective, intuitive templates/style sheets for site standardization and to simplify changes.
Prepares artwork for the web using hardware/software tools associated with the creation of artwork. Keeps up to date with developments in web design theory, practice and technology.

STYLE GUIDE FOR USCG WWW WEBMASTERS

I. PURPOSE

The purpose of this style guide is to assure:

- (1) a clear and consistent U.S. Coast Guard (USCG) identity on all official WWW pages;
- (2) a consistent and predictable navigation approach on all official WWW pages;
- (3) consistency with all Coast Guard strategic communication efforts.

Requirements are kept minimal to achieve the above objectives while leaving considerable room for program and regional creativity and style. Programs, Areas, MLCs and Districts are encouraged to develop consistent style guidelines appropriate for their AOR within the limits of overall USCG guidelines.

II. SCOPE

Many books provide information on web page design best practices. This guide will limit itself to essentials for official USCG WWW pages.

A. WEB PAGE BASICS

1. The Home Page (major directory or index).

The term Home Page, as used in this style guide, refers to the main index or directory of pages for the U.S. Coast Guard, Assistant Commandants/Programs, Areas, MLCs, and Districts only.

Home Page requirements:

All Home Pages shall have the CG banner at the top.

"Operation Value" (see Commandant Notice 5726, December 31, 1996) or strategic messages shall be incorporated below the large banner along with or below the Program, Area, or District title, graphic or logo.

The CG rod shall be placed at the bottom of the page.

All space between the CG banner and CG rod can be used at the discretion of the webmaster.

Below the rod shall be: (1) a link to the [USCG Home Page], the format is [USCG Home Page] (2) an e-mail address for webmaster [webmaster@www.uscg.d1.mil] below the [USCG Home Page] link

Enclosure (2) to COMDTINST 5230.56

and 3) a created and/or update date [Updated: January x, 19xx] below the e-mail address. Nothing else shall be placed below the rod.

2. Lead Page (index to specific content section under a Home Page).

Some web pages, while not being a Home Page, are lead index pages to a content section. Each Lead Page to a content section shall provide an e-mail address for CONTENT related questions.

Lead Page requirements:

All Lead Pages shall have the CG banner at the top.

All Lead Pages shall have the CG rod at the bottom.

All space between the banner and rod can be used at the discretion of the webmaster.

Immediately below the rod shall be a link to the appropriate Assistant

Commandant, Area or District home page, as well as the USCG Home Page.

The e-mail link for a content contact shall be placed below the District/Area/Program link.

A Created and/or Updated date shall be placed below the e-mail address.

Nothing else shall be placed below the rod.

3. Web Pages.

All pages other than Home Pages or Lead Pages are referred to as web pages.

Web Page requirements:

All web pages shall have a CG banner at the top. (Exceptions can include a single graphic, a photograph, or some document reproductions.)

The CG rod shall be placed at the bottom of the web page.

All space between the CG banner and CG rod can be used at the discretion of the webmaster.

Below the small rod shall be a link to the Assistant Commandant, Area or District home page, as well as the USCG Home Page.

A Created and/or Update date shall be placed on the first page of each separate content section below the Program and District or Area links.

An e-mail address [content@comdt.uscg.mil] for the content contact shall be placed below the Program/Area/District link.

Nothing else shall be placed below the rod.

All web pages shall provide a link back to the Lead Page immediately ABOVE the CG rod.

B. CONTACTS: ADDRESSES, TELEPHONE NUMBERS AND FAX NUMBERS

All addresses, telephone numbers and fax numbers shall be placed ABOVE the CG rod.

Personnel listings shall consist of only those contacts needed by the public and refer to positions and titles, rather than personal names of staff members.

C. TEXT ALTERNATIVES

All graphic navigational devices and image maps shall have a text alternative.

All non-text elements shall have an alt tag.

All pages using frames, motion graphics, java and similar enhancements shall provide a plain text alternative.

Content shall be made available to users with text readers.

D. LINKS AND NAVIGATION

External links to other military, government and educational institutions are authorized.

External links shall directly support the objective of the page content.

Links to commercial vendors and other private pages shall have an essential business justification and be reviewed for legal implications.

Links are extensions of content and shall be approved by the content approval official.

(Keep in mind that the decision to link to one external site may require linking to all similar sites and laws on linking issues are evolving.)

Approved links to external sites shall include links to a local copy of the standard DOT disclaimer once it is developed. In the interim, pages with external links shall include the following disclaimer:

"Links from these pages/this page to non-Coast Guard sites do not represent any implicit or explicit endorsement by the United States Coast Guard of any commercial or private issues or products presented there."

Links shall be regularly monitored and maintained by the webmaster.

All links designed in graphic format shall have a text alternative.

Review **A.WEB PAGE BASICS**, sections 1, 2 and 3 for Home Page, Lead Page and Web Page link requirements.

Use relative URLs , rather than fixed URLs for links to pages on the USCG WWW server (i.e.www.uscg.mil).

Use:

Do not use:

Enclosure (2) to COMDTINST 5230.56

Using relative URLs will allow the movement of the entire "directory tree" of HTML code to another server and the code will continue to operate without modification.

E. FILE NAMES

All lower case letters are recommended for file names to promote cross platform recognition.

```
+-----+
| NOTES:                                     |
|                                           |
|     USCG WWW pages that do not conform to the above standards will |
|     either be modified or removed, at the discretion of the ICCB. |
|                                           |
|     An Internet Toolbox with page templates, graphic elements, a |
|     registration form, style guide and policy will be located on |
|     the CG Web.  Until all units have access the interim location |
|     will be:  http://www.uscg.mil/tools/index.html |
|                                           |
|     Address all concerns about this style guide to the ICCB. |
+-----+
```

Enclosure (3) to COMDTINST 5230.56

Coast Guard Internet Security Plan
To be developed by G-SII and OSC

Coast Guard Internet Training Plan

Training can be broken down into three levels. The levels, training recommendations and estimated costs (as of June 1997) are included below. Units are responsible for funding their own training.

LEVEL	JOB DESCRIPTION	RECOMMENDED TRAINING	ESTIMATED COST
Content Provider	Authors and/or provides official approved content for publication on the Internet	MS Word with Internet Assistant and basic HTML course	\$1000 per year per person
Content Approval Official	Provides oversight for content providers. Establishes broad content priorities and guidelines. Manages web content within their area of responsibility. (typically at the Office level, District/MLC/Area Division level) Takes editorial responsibility for the content Ensures web area performance measures are clearly established and maintained. Ensures compliance with all relevant laws and policies.	MS Word with Internet Assistant advanced HTML course, Front Page training, content management course (consisting of FOIA training, Privacy Act training, Public Affairs training, Basic Security Training).	\$2000 per year per person
Web Masters	Person who manages a website; mediator between content approving officials and system administrator; ensures that applicable standards such as HTML validity and link liveness are met, optimizes the web architecture for navigability, takes responsibility for the quality and style of the site; develops and enforces the website's style; liaises with graphic artists; provides first level of user support: creates web pages for other offices that do not have adequate resources to devote to web page production. Ensures compliance with all relevant laws and policies.	Front Page training, advanced HTML course, IIS training, Basic Security Training, Web Graphics Design	\$5000 per year per person

Note: The first two levels will probably be filled by Coast Guard personnel although the task of content provider can be outsourced under the right conditions. If content provider and/or web master responsibilities are outsourced, then these costs are not applicable as they should be included in the outsourcing fees.

Enclosure (5) to COMDTINST 5230.56

Government Information Locator Service (GILS) Requirements

GILS requirements are currently being revised and updated by the Office of Management and Budget (OMB). Additional policy will be added to this section upon OMB's release of the updated requirements.

Internet Support Plan

To be developed by OSC upon awarding of Internet Support Contract.

NOTE: The following is from the CGWEB instruction:

Costs Planning

Support requirements for Internet web-related activities will vary, increasing over time as the Internet is more fully utilized. Necessary resources and configuration management are presented to clarify issues and requirements.

(1) Required System Support Services.

Resources listed in the table below are necessary for any facility supporting Intranet activities. Depending on the size and need of the facility, personnel resource types may be consolidated or expanded. As an example, a facility that requires 24x7 service will need to add resources in both Network and System Administration. An additional Webmaster may be necessary if system expansion exceeds present capabilities.

RESOURCE TYPE	DESCRIPTION	COST/HOUR (contracted range)
NETWORK ADMINISTRATION	TISCOM provides Network Management (e.g. planning) services. Additional tasks include: Router programming/administration Firewall programming/administration LAN connectivity/administration WAN connectivity Security Services	\$55-110/HOUR Dependent upon skill level and contract utilized.
SYSTEM ADMINISTRATION	A majority of larger units will have a dedicated staff of administrative personnel. Their tasks include: Operating system installation, upgrades, maintenance. Application installation, upgrades, maintenance. System tuning, performance enhancements. Systems Security	\$40-85/HOUR Dependent upon skill level and contract utilized.
SITE-MANAGER	A Internet Site Manager's responsibilities include: Management of configurations for all Web-related systems and their architecture.	\$65-120/HOUR Dependent upon skill level and contract utilized.

Enclosure (6) to COMDTINST 5230.56

	Management of timely and orderly updates and system revisions.	Services may be provided by Coast Guard or government personnel.
	Coordination of network and system services and personnel.	
	Resource projections and system expansion.	
	Funding projections and allocations.	
	Web Security Management	
WEB MASTER(S)	A Web Master's responsibilities include:	\$40-85/HOUR
	Coordination, review, development and management of an Internet site.	Skill level and location.
CONTENT OVERSIGHT	Content oversight responsibilities include:	Government personnel, collateral duty (depending on size & complexity of web area).
	Establishment, maintenance, and enforcement of priorities, guidelines and directives.	
CONTENT PROVIDER	Content oversight responsibilities include:	\$30-85/HOUR
	Author/provide content for publication.	Skill level developer or author), Collateral duty. Can be outsourced.
	Analyze and develop applications.	
	Update published documents and applications in a timely manner.	
	Comply with guidelines & directives	

Many tasks can be consolidated. A Network Administrator may also be a System Administrator. Site-Managers may also be Web Masters, and may provide as well as manage content.

The cost/hour specified are based upon a review of available contracts and relative locality costs. Skill level needs will represent the largest individual cost variance. Facility size, needs, and activities are primary cost determinants.

Enclosure (7) to COMDTINST 5230.56

Coast Guard Internet Configuration Management Plan

To be developed by OSC Martinsburg upon awarding of CG Internet Support Contract.

INTERNET PERFORMANCE MEASUREMENT GUIDELINES

Several methods can be used to measure the value of information distribution using the Internet. The methods allow flexibility to meet program specific criteria. Each method measures a different aspect of web performance. Taken together, these methods provide an estimate of the effectiveness of a CG WWW site.

1. QUALITATIVE MEASURES

Each CG WWW content section shall provide a mechanism for user feedback. The Internet is a medium that provides an easy and instant way for users to express general concerns and request additional information and services in response to web site content and technical issues. A hyperlink to an e-mail address is the minimum requirement.

A systematic approach to tracking e-mail messages will enable programs to take maximum advantage of the opportunity to measure and improve their Internet presence and customer service as well as provide cost savings to the program and the organization. E-mail can be sorted into predetermined categories. Suggested categories include:

- Content Requests
- Content Corrections and Complaints
- Technical Problems
- One Time Requests for Information
- General Comments

Additional categories can be added to accommodate other specific measurement criteria as needed.

Note: requests for Coast Guard records via the internet are not valid FOIA requests. Any request for Coast Guard records from a non- Governmental entity received via the world-wide web should be returned to the sender with instructions on the appropriate method to file a FOIA request.

2. QUANTITATIVE MEASURES

Another method for measuring traffic to the web site is to evaluate the web site access statistics or "hits". These statistics give an account of total web site files transmitted monthly, daily, and also provide averages. Hit counts can indicate where traffic sources originated. However, hit counts are a very imperfect measure. One page can count as five hits if it contains four graphics. Each page element counts as a hit. Therefore, the number of page elements must be divided into the total hit count for that page. Furthermore, hits give no indication of why the hit was made.

The page could have been inadvertently accessed. Finally, each page or section can be evaluated for access times. Time of access can provide some indication of the type of users accessing the page and why they are accessing the page.

The "hit" measurement method is best used to gauge broad trends over time. Feedback from users, when used in conjunction with this information, can keep a website more responsive to its users' needs.

3. **COMPARISON MEASURES**

Although the Internet is only one of many communications mediums, it has the potential to deliver more efficiently and with less cost than traditional means. For example, documents, once posted on the web server, can be downloaded indefinitely by web site customers without requiring additional program time and/or funds for duplicating and packaging the documents for each request. A comparison approach to web site measurement will enable each web content author to contrast resource expenditures using traditional distribution methods with that of the Internet.

REGISTRATION - PART A

For a U. S. Coast Guard WWW Site

PURPOSE

The purpose of this recommended registration is to provide accountability and essential information needed to manage a Coast Guard WWW site. It should be submitted to and kept by the WWW content approval official for an Assistant Commandant Program, Area, MLC or District. Submit one Part A registration for each separate content section or content author within a web site.

PART A-1. CHECKLIST FOR THE CONTENT AUTHOR

1. Summarize the business objective of your proposed web site.

2. Who will be the KEY customer? _____

3. Why is the WWW the best means to convey your information or service?

4. How will your web presence reduce costs and improve business processes and customer service for the U.S. Coast Guard and the American taxpayer?

5. Will this be the ONLY copy of your content? If yes, consult COMDTINST 5212.12 to determine its record disposition. Make a copy and save it.

6. How frequently will your content need updating? _____

7. Does your site contain necessary metaheaders (hidden keywords for web search engines) to properly identify it to internal and external customers? _____

DEPT. OF TRANSP., USCG CG - 5641 (12/97)

Enclosure (9) to COMDTINST 5230.56

8. What is the long term plan to maintain and update your web content? Are staff time and or funds available _____

9. What is your plan for responding to e-mail generated by the web site? Note FOIA request procedures (see reference (b) and enclosure 8 of this instruction) _____

10. What measurement criteria will you use to assess web site goal achievement? _____

11. Will posting these web pages or providing this web service require additional capabilities, resources or funding? (i.e. staff, databases, restricted access, special server, etc.) _____

12. Name of content release official
Signature _____
The above signature indicates that the proposed WWW content has been reviewed for subject and grammatical accuracy and is approved for release.

PART A-2. CHECKLIST FOR THE ASSISTANT COMMANDANT PROGRAM, AREA, MLC OR DISTRICT WWW CONTENT APPROVING OFFICIAL

1. Does the proposed content in Part A-1 contribute to an overall balanced web presentation for the Assistant Commandant Program, Area, MLC or District?

2. Is the content compliant with:
a) Internet Instruction, COMDTINST 5230.56 _____
b) Paperwork Management Manual, COMDTINST M5212.12 _____
c) Public Affairs Manual, COMDTINST M5728.2B _____
d) Freedom of Information and Privacy Acts Manual, COMDTINST M5260.3 _____
3. Is the content appropriate for a national and international community?

4. Will placing these web pages or providing this web service require additional capabilities, resources or funding? (i.e. staff, databases, restricted access, special server, etc.)

5. Priority level assigned by Assistant Commandant Program, Area, MLC or District WWW Content Approving Official.
HIGH ____ MEDIUM ____ LOW ____ NOT ACCEPTED ____
6. Name and signature of Assistant Commandant Program, Area, MLC or District WWW Content Approving Official
Name: _____
Signature: _____
7. Submit a copy of this form to the appropriate webmaster.

Enclosure (9) to COMDTINST 5230.56

REGISTRATION - PART B

For a U. S. Coast Guard WWW Site

PURPOSE

The purpose of this required registration is to provide accountability and essential information needed to manage a Coast Guard WWW site.

PART B-1. FOR THE WWW CONTENT APPROVAL OFFICIAL

Area of responsibility (AOR) (i.e. District, Headquarters, Program, Area, MLC)

State the overall business objective of the WWW site.

What special resources are needed (i.e. databases, secure access, special server etc.)

Name of WWW content approval official _____

Signature _____

The above signature indicates that I assume overall responsibility for the direction and approval of content for the web sites within my AOR.

PART B-2. FOR THE WEBMASTER

1. Area of responsibility (i.e. District, Headquarters. Program, Area, MLC)

2. Name of Webmaster: _____
e-mail: _____
telephone: _____

3. Signature _____
The above signature indicates that I take responsibility for adherence to all Coast Guard Internet policies and guidelines for technical criteria, style and appearance.

4. **SEND A COPY OF THIS COMPLETED REGISTRATION -PART B (PARTS I AND II) TO THE INTERNET CONFIGURATION CONTROL BOARD (ICCB) FOR WWW RESOURCE AND CONTENT REGISTRATION.
THE ICCB ADDRESS IS:**

**USCG, Commandant (G-SIA), 2100 2nd Street SW, Washington, DC 20593,
Attn: ICCB.**

PROCESS FLOWCHART FOR WWW PUBLISHING

WWW Site Planning for the Content Author

- Summarize business objectives.
- Identify KEY customers and stakeholders.
- Assess how a WWW site will facilitate achieving business objectives and reaching Key customers and stakeholders.
- Will you need to create new material or reformat existing material?
- How should you present your material so that it is useful and appealing to your key customers.
Example: Do the some of your customers want text only information for text only browsers?
- Who will be responsible for web content and web page development?
- Who will be responsible for updating web content?
- How will a WWW site reduce costs, improve business processes and customer service?
- Will the WWW site require extensive maintenance or special hardware and software?
- How often will the content need updating?
- Are you familiar with applicable CG policy and law such as: Copyright, Freedom of Information and Privacy Acts, CG Internet policy?
- Do you have a plan for answering WWW e-mail?
- Have you identified the measurement criteria that will assess business goal attainment?



Continued on next page...

